스마트 그리드 내의 비인가 기기를 이용한 개인정보 위협에 관한 연구

강보선, 이근호, 윤성현
백석대학교 정보통신학부
masati@bu.ac.kr, root1004@bu.ac.kr, shyoon@bu.ac.kr

A Study of Personal Information Threats using Unauthorized Devices in Smart Grid

Bo-Seon Kang, Keun-Ho Lee , Sunghyun Yun
Division of Information and Communication, Baek-Seok University

요 약

M2M기술의 발전으로 새로운 기술들이 생겨나고 있다. 그중에서도 에너지를 능률적이고 보다 안전하게 운용할 수 있게끔 해주는 스마트 그리드에 대한 개념과 지금 현재 스마트 그리드 보안 위협에 대해 살펴보자. 보안 위협 시나리오를 수립한 다음 정보통신 사회에서 보다 안전하고 능률적인 보안 대응 방안을 체계적으로 분석한다.

1. 서론

스마트 그리드는 전력망의 효율성을 증대하기 위한 방법으로 개발하는 방법마다 규격과 방식이 모두 다르지만 스마트 그리드를 이용하는 공통된 목적은 모두 같다고 생각한다. 스마트 그리드를 사용하는 목적은 광범위한 정전사고를 피하기 위하여, 끊임없고 안정된 전기 흐름을 제공하기 위하여 전력 공급 중단으로부터 회복이 가능해야하며 자연재해와 극단적인 날씨와 인공 파손과 같은 긴급상황에서도 전기 그리드를 평상시와 동일하게 안전한 운영을 보장해야하고 자동 복구능력을 제공 할 수 있어야한다[1]. 하지만 누군가 악의를 가지고 모든 전력망과 소비자가 연결되어있는 네트워크에 침입하여 관리자 계정을 탈취하여 차단시킨다면 스마트 그리드 전력망은 그 순간 모두 다운 될 수도 있을 것이다. 그렇다면 네트워크를 통해 스마트 그리드에 사용되는 개인정보와 과금 정보 등 중요 정보가 넘어 갈 것이다. 실제로 2009년에 푸에르토리코에서 스마트미터기가 해킹당하는 사건이 발생해서 피해액이 3400만 달러에 이른다고 한다. 그렇기에 더 이상 피해가 발생하지 않고, 스마트 그리드가 안전하게 자리를 잡기 위해서는 시스템 보안망을 구축 하여야 한다.

녹색정상위원회의 로드맵 중에는 2030년까지 국가단위의 스마트 그리드를 구축할 전망이라고 한다[2]. 어느 IT 분야에서나 보안은 중요하지만 국가 단위의 스마트 그리드의 보안은 그 중요도가 매우 높다고 생각 한다. 다른 국외의 스마트 그리드 보안 기술에 비해 조금 뒤쳐져있는 것은 사실이지만 차이는 미비하여 보안의 기반을 다잡고 기술을 잘 개발 운용한다면 세계시대의 중심의 스마트 그리드 기술이 될 수 있을 것이다.

2. 스마트 그리드 보안

현재의 스마트 그리드 기술은 보기에 에너지문제를 해결해주고 새로운 미래의 기술일수도 있다. 또한 전력망의 효율성을 증대시켜주는 미래기술일수도 있다. 하지만 신기술의 등장은 항상 악용하려고 하는 존재들의 등장으로 언제 어디서나 위협을 받고 있다. 스마트 그리드로 점차 나아가면 이전에 있던 전기 그리드의 네트워크는 상호 연결을 염두에 두어 두지 않았으므로 반드시 새로운 위험과 마주하게 될 것이다.

2.1 스마트 그리드 보안 위협

스마트 그리드에서 보안에 신경 써야 하는 부분을 나누어 보자면 서비스 부분 , 네트워크 부분, 단말 부분, 가입자 부분으로 분류하여 정리할 수 있다[3]. 서비스 부분은 스마트 그리드의 서비스 제공자에 속하는 서버와 운영 정보 같은 것들을 포함하고, 네트워크 부분은 네트워크 제공자에 속하는 라우터나 스위치 등 물리적 장비와 네트워크 자원이라고 볼 수 있다. 단말 자산은 사용자의 단말기를 의미 한다고 볼 수 있다. <표 1>처럼 스마트 그리드의 보안 위협 요소들은 다양한 방면에서 볼 수 있다. 또한 스마트 그리드를 구성하는 다양한 기기들 중 보안 대상에 포함되지 않거나 보안이 상대적으로 허술한 기기들은 공격자의 위험에 노출 될 수밖에 없다. 만일 펌웨어 보안이 취약한 기기를 공격자가 아이폰의 탈옥과 같이 펌웨어를 조작하여 설정을 모두 풀어버리고 공격자의 마음대로 조작한다면 전기요금뿐 아니라 장치내의 모든 정보가 유출 될 수 도 있다.

<표 1> 스마트 그리드에서의 보안 위협의 종류

구분	서비스 보안 위협
종류	•스마트그리드의 서비스 서버를 공격하여 서버자원을 고갈시킴으로써 합법적인 가입자의 서비스를 방해 •스마트그리드 서버에 불법적으로 접근 •서버 세션의 상태를 훔치거나 도용 •악성코드를 감염시켜 정상적인 동작 방해와 정보 유출 •서버에 송수신되는 정보 및 저장된 정보를 불법적으로 획득 •서버가 취급하는 정보를 위변조
	네트워크 보안 위협
	•네트워크 자원을 고갈 시킴으로써 합법적인 가입자의 서비스 이용 방해 •고객 도메인 구성 요소의 세션 상태를 훔치거나 도용 •스마트그리드 구성 요소에 송수신되는 정보 및 저장된 정보를 불법적으로 획득
	단말 보안 위협
	•고출력 전자기파를 방사하여 스마트 기기를 파괴 •스마트그리드 기기의 패스워드를 추측하거나 을을 프로그램 취약점을 이용하여 스마트그리드 기기에 침입 •기기의 보안 정보를 공격자가 기기에 저장하여 기기 복제 하거나 스마트 그리드 기기 정보를 변경하여 기기 위변조 •스마트그리드 구성 요소로 위장하여 불법적인 제어 명령 전송 •스마트그리드 구성요소가 취급하는 정보를 위변조

3. 스마트 그리드 구성 기술

스마트 그리드를 가정까지 끌어오기 위해서는 개개인의 가정집에도 스마트 그리드 기기를 설치해야한다. 이때 스마트미터기를 사용한다. 스마트미터기는 디지털미터기라고도 불리며 분전반이나 배전반에 설치하여 에너지의 사용량을 효율적으로 측정해주는 기기이다. 가정에서 사용하는 에너지를 측정하여 측정한 정보를 바탕으로 에너지사용요금을 정산해준다. 초창기에는 단순한 에너지 사용량과 요금을 보여주었지만 나아가 실시간 정보제공뿐 아니라 과거에 사용했었던 에너지양을 통계분석하고 사용자에게 다양한 정보 서비스를 제공하는 역할까지 담당하고 있다.

4. 비인가 기기를 이용한 공격 시나리오

현재 나와 있는 스마트미터기는 개인 사용자가 마음대로 에너지양을 조절하지 못하도록 암호화 되어있다. 하지만 이러한 스마트미터기의 암호화는 반드시 있는 취약점을 통해 풀리게 된다[4]. 이때 작게는 사용자의 에너지양을 '0' 으로 만들어 에너지를 아무리 사용해도 비용이 나오지 않게 할 수도 있다. 하지만 스마트 그리드는 네트워크를 사용하기 때문에 공격자의 마음대로 움직일 수 있는 스마트미터기는 언제든지 공격할 준비가 되어있는 상태이다.

스마트 그리드는 항상 운영센터와 개인의 스마트미터기와의 정보 송수신을 중요시 한다[5]. 그래야만 효율적인 전력망을 구성 할 수 있기 때문이다. 이때 이점을 이용하여 비인가 된 공격자의 스마트미터기를 스마트 그리드에 연결하고 에너지사용량으로 위장한 악성코드를 운영센터로 전송한다[6]. 그 다음 운영센터와 연결하고 있는 사용자들의 개인정보를 모두 탈취하여 요금을 공격자의 마음대로 설정 할 수도 있다. 공격자는 자신이 속해있는 전력망 내의 모든 스마트미터기를 점유하면 개인의 한 장소의 문제가 아니라 건물, 지역 나아가 스마트 그리드를 구성하고 있는 모든 요소들에게 영향을 끼칠 수 있을 것이다. 공격자는 사용한 스마트미터기에 담는 악성코드의 내용에 따라서 국가의 중요한 시설이 되는 발전소 같은 중요 시설을 공격할 기회도 가져가므로 대응 방안이 필요한 시점이다.

5. 대응방안

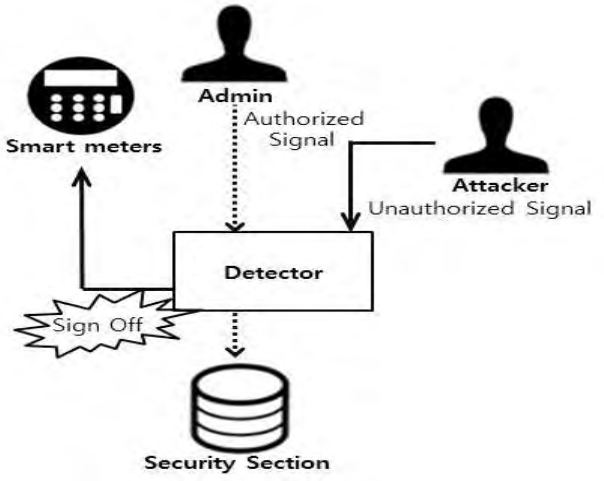
현재 스마트 그리드 보안을 위한 준비를 다양한 기업들이 하고 있다[7].

<표 2> 각 기업별 보안

	분야	보안고려사항	요구사항
CISCO	Network	기존 장치 고려	Customer Operation
JUNIPER	Network	취약점	방화벽
CURRENT	Network	인증, 원격접속	암호, 접근통제
HP	AM (평가)	취약점 식별	침투 테스트

기업들도 주로 네트워크의 취약점에 대한 방향으로 보안위협을 대비하고 있다. 그만큼 스마트 그리드에서 네트워크에 대한 보안 취약점은 대단히 중요한 부분이라고 볼 수 있다.

스마트미터기를 통한 운영센터의 공격 시나리오를 막는 방법으로는 첫 번째, 스마트미터기를 분석하지 못하도록 막아두는 것이다. 암호를 해독하기 위해서는 PC에 연결하여 프로그램을 실행시켜야하는데, 이때 PC에서 스마트미터기의 암호를 해독하기 위한 방법으로는 여러 가지가 있다. 방법이 여러 가지여도 항상 스마트 미터기의 암호담당 구획을 목표로 한다. 암호 구획에 인가 받지 않은 방식의 신호가 접근할 때 신호를 탐지하는 알고리즘을 추가하여 비인가 신호를 탐지 한다면 스마트 미터기의 작동을 중지시킨다. 작동을 중지시키더라도 사용자가 사용한 에너지의 양의 정보를 잃지 않고 정상 작동 하는 것이 관건이다.



(그림 1) 스마트미터기의 보안 구획 신호탐지

두 번째, 운영센터로 들어가는 방화벽에 사용자가 사용하는 에너지양의 패킷 정보를 한 번 더 분석하는 방화벽을 설치한 다음 스마트미터기의 패킷 정보를 간소화 하여 최소한의 정보를 담도록 하여 용량이 커지면 아예 송수신 자체를 안 되도록 막는 방법이 있다.

6. 결론

스마트 그리드는 에너지를 효율적으로 관리하도록 도와주기 때문에 좀 더 나아가면 전력망을 모두 연결하여 비교적 적은 자원으로 에너지를 생산하여 효율적으로 사용할 수 있을 것이다. 하지만 현재에는 도입하는 단계이기 때문에 취약점이 존재 할 수밖에 없다. 일반의 전력망에 ICT 기술을 접목하는 방식인 스마트 그리드는 개인 정보에도 관심을 반드시 가져야 한다. 네트워크상에서만 중시되었던 기밀성, 무결성, 가용성은 이제 전력망이 네트워크와 합쳐지면서 같이 생각해 봐야할 문제다. 소비자에 대한 보안 위협을 막아줄 보안대책과 국가에서 나서서 정책을 마련하고 도와줘야 하는 것에 최선을 다해야지 스마트 그리드의 장점 중 하나인 '고장 전 예방' 의 이점을 살릴 수 있을 것이다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348). 또한 '산학협동재단'지원으로 수행된 연구임.

참고문헌

[1] 이일우, "정보통신기술 관점에서의
스마트 그리드 참조 모델", TTA, TTAR-04.0001, 2012.
[2] 도윤미, "스마트 그리드 기술 동향 : 전력망과
정보통신의 융합기술", ETRI, Vol. 24, No. 5, pp.74-86, 2009.
[3] 김미주, "스마트 그리드 시스템 보안 기능 요구 사항", TTA, TTAR.KO-12.0209, 2012.
[4] 토니 플릭, "스마트 그리드 보안", 비제이퍼블릭, 268p
[5] 이건희, "스마트 그리드 보안위협 및 보안 요구사항 분석", 정보보호학회, Vol. 2, No. 7, pp.7 - 17, 2011.
[6] 유성민 외 2명, "스마트 그리드 보안기술 동향분석 및 대응 방안", 한국통신학회 논문지, Vol. 31, No. 5, pp.8-14 2014.
[7] 정영곤 외 2명. "스마트 그리드 보안 동향", 정보보호학회지, Vol. 20, No. 4, pp.66 - 79, 2010.